TLP:WHITE

SICK PSIRT
Security Advisory

OpenSSL vulnerability affects multiple SICK SIMs

Document ID:	SCA-2022-0012
Publication Date:	2022-08-03
CVE Identifier:	CVE-2022-0778
CVSSv3 Base Score:	7.5
CVSSv3 Vector String:	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Version:	3

Summary

In March 2022, the OpenSSL development team disclosed a denial of service in versions ”3.0.0,” ”3.0.1,” ”1.1.1”-”1.1.1m” and ”1.0.2-1.0.2zc” of the OpenSSL library. Exploiting this vulnerability allows remote, unauthenticated attackers to cause an infinite loop. It is possible to trigger the infinite loop by creating a certificate that has invalid explicit curve parameters or when parsing created private keys, as they may contain explicit elliptic curve parameters. It may be possible to put the SIMs in a non-responsive state since 100% of the CPU resource is consumed by the infinite loop calculation. The listed SICK SIM products are currently operated with an OpenSSL version that is vulnerable to CVE-2022-0778. With that it could be possible to exploit the mentioned vulnerability if the SIM devices are connected to a network with untrusted devices. In that case an untrusted client may send a manipulated SSH-certificate to the SIM, which exploits the vulnerability in the OpenSSL library as described above when it comes to the certificate validation by the SIM product. Evaluation is undergoing.

List of Products

Product	Part Number	Affected by
SICK SIM1000 FX with Firmware <= 1.5.2	1097816 1097817	CVE-2022-0778 Status: Known Affected Remediation: Workaround, None available
SICK SIM1004 with Firmware <= 1.1.0	1098148	CVE-2022-0778 Status: Known Affected Remediation: Workaround, None available
SICK SIM1012 with Firmware <= 2.0.6	1098146	CVE-2022-0778 Status: Known Affected Remediation: Workaround, None available
SICK SIM2000-2 P Track & Trace with Firmware <1.7.0	1117588	CVE-2022-0778 Status: Known Affected Remediation: Vendor fix
SICK SIM2000ST Track & Trace (2086501) with Firmware <= 1.7.0	2086501	CVE-2022-0778 Status: Known Affected Remediation: Workaround, None available
SICK SIM2000ST Track & Trace (2086502) with Firmware <= 1.13.2	2086502	CVE-2022-0778 Status: Known Affected Remediation: Workaround, None available
SICK SIM2000ST with Firmware <= 1.7.0	1080579	CVE-2022-0778 Status: Known Affected Remediation: Workaround, None available
SICK SIM2000ST-E with Firmware <1.7.0	1112345	CVE-2022-0778 Status: Known Affected Remediation: Vendor fix
SICK SIM2x00 with Firmware <1.2.0	1081902 1092673 1112341	CVE-2022-0778 Status: Known Affected Remediation: Vendor fix

SICK SIM4000 with Firmware <= 1.10.1	1078787 1078484 1084131	CVE-2022-0778 Status: Known Affected Remediation: Workaround, None available

Vulnerability Overview

CVE-2022-0778 Loop with Unreachable Exit Condition ('Infinite Loop')

CVE Description: Description of the original advisory from OpenSSL: "The OpenSSL BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial-of-service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters."

CVE-2022-0778 has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-835 (Loop with Unreachable Exit Condition ('Infinite Loop'))

References:
OpenSSL Security Advisory:
https://www.openssl.org/news/secadv/20220315.txt

CVE Entry:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0778

Remediations

Vendor Fix for CVE-2022-0778

Details: The recommended solution is to update the firmware to a version >= 1.2.0 as soon as possible.

Valid for:

- SICK SIM2x00 with Firmware <1.2.0

Details: The recommended solution is to update the firmware to a version >= 1.7.0 as soon as possible.

Valid for:

- SICK SIM2000-2 P Track & Trace with Firmware <1.7.0
- SICK SIM2000ST-E with Firmware <1.7.0

Workaround for CVE-2022-0778

Details: In the runtime context of an SIM application, the SSH access should not be required at all, it is recommended as a workaround to disable port 22 (SSH) of the corresponding Ethernet port at the SIM via App (Firewall-API).

Valid for:

- SICK SIM1000 FX with Firmware <= 1.5.2
- SICK SIM1004 with Firmware <= 1.1.0
- SICK SIM1012 with Firmware <= 2.0.6
- SICK SIM2000ST Track & Trace (2086501) with Firmware <= 1.7.0
- SICK SIM2000ST Track & Trace (2086502) with Firmware <= 1.13.2
- SICK SIM2000ST with Firmware <= 1.7.0
- SICK SIM4000 with Firmware <= 1.10.1

None available for CVE-2022-0778

Details: The recommended solution will be the update of the firmware to a version >= 1.10.2 (release not yet scheduled). Please see “Workaround”.

Valid for:

- SICK SIM4000 with Firmware <= 1.10.1

Details: The recommended solution will be the update of the firmware to a version >= 1.7.1 (release not yet scheduled). Please see “Workaround”.

Valid for:

- SICK SIM2000ST Track & Trace (2086501) with Firmware <= 1.7.0
- SICK SIM2000ST with Firmware <= 1.7.0

Details: The recommended solution will be the update of the firmware to a version >= 1.13.3 (release not yet scheduled).

Valid for:

- SICK SIM2000ST Track & Trace (2086502) with Firmware <= 1.13.2

Details: The recommended solution will be the update of the firmware to a version >= 2.1.0 (in progress, release not yet scheduled).

Valid for:

- SICK SIM1012 with Firmware <= 2.0.6

Details: The recommended solution will be the update of the firmware to a version >= 2.0.0 (in progress, release not yet scheduled).

Valid for:

- SICK SIM1004 with Firmware <= 1.1.0

Details: The recommended solution will be the update of the firmware to a version >= 1.6.0 (in progress, release not yet scheduled).

Valid for:

- SICK SIM1000 FX with Firmware <= 1.5.2

General Security Practices

General Security Measures

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Vulnerability Classification

SICK performs vulnerability classification by using the CVSS scoring system (*CVSS v3.1*). The environmental score is dependent on the customer's environment and can affect the overall CVSS score. SICK recommends that customers individually evaluate the environmental score to achieve final scoring.

Resources

SICK PSIRT Security Advisories:
https://sick.com/psirt

SICK Operating Guidelines:
https://www.sick.com/media/docs/9/19/719/special_information_sick_operating_guidelines_cybersecurity_by_sick_en_im0106719.pdf

ICS-CERT recommended practices on Industrial Security:
http://ics-cert.us-cert.gov/content/recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

History

Version	Release Date	Comment
1	2022-08-08	Initial Release
2	2023-02-10	The canonical URL.
3	2025-07-30	Updated Advisory: URL for SICK Operating Guidelines has been updated